Course Description

Analyzing Malware

Intel® Security Foundstone® Services Training Course

Malware attacks are often mistaken as system or network problems, often resulting in overlooked incidents that allow attackers to burrow deeper into environments and gain increased access over time. The goal of this class is to better prepare you to respond to malware incidents in a structured, effective way—so you can improve detection, containment, and eradication. You will learn how to build a malware analysis toolkit and pick apart file-based threats attempting to hide or protect themselves through a variety of hiding, obfuscation, and anti-debugging techniques. The lessons learned during this class can aid an incident response (IR) program by equipping your team with a robust malware analyst capability, a required component of a proactive threat hunting program.

Course Goals

- Identify and respond to attacks.
- Conduct forensically sound investigations.
- Analyze malware and understand economy.
- Incorporate threat hunting on your system.

Agenda At A Glance

- Malware Ecosystem
- Lab Setup
- Windows Forensics
- Memory Analysis
- Network Forensics
- Malware Delivery Vectors
- Malware Analysis
- Automation and Hunting

Audience

This course is intended for system and network administrators, corporate security personnel, auditors, law enforcement officers, and consultants responsible for investigating malware outbreaks or network investigations.

intel Security

Course Description

Recommended Pre-Work

Basic understanding of UNIX, Windows OS, computer forensics, and TCP/IP networking is required for the course to be fully beneficial.

Course Outline

Module 1—Malware Ecosystem

- Definition
- Malware History
- Malware Economy
- Incident Response
- Malware Classification
- Infection Vectors
- Antivirus

Module 2—Lab Setup

- Anonymize Your Activities
- Set up a Malware Lab
- Honeypot
- Sandboxing
- Manage Your Zoo

Module 3—Windows Forensics

- Process/Methodology
- File System
- Acquisition
- Windows Artifacts
- Malware Incident Response

Module 4—Memory Analysis

- Understanding Memory
- Dumping Memory
- Introduction to Volatility
- Windows Memory Forensics

Module 5—Network Forensics

- Research Domains and IPs
- Malware Networking (Topology, Fast Flux, DGA, DNS Tunneling)
- Network Signature and Patterns (Snort, Wireshark)
- Scapy, TraceWrangler

Module 6—Malware Delivery Vectors

- Attack Vectors
- PDF Obfuscation Techniques
- Malicious Office Documents
- Malicious SWF Analysis

Module 7—Malware Analysis

- Structure of a Portable Executable (PE)
- Windows API
- Malware Protection (Packer, Anti-Debug, Anti-Sandbox, Escalate Privilege)
- Static Analysis
- Dynamic Analysis
- Profiling Malware
- Hunting Malware in Memory

Module 8—Automation and Hunting

- Triage Evidence
- Writing Yara Rules
- Automation
- Rastrea2r

To order, or for further information, please call 1 888 847 8766 or email **SecurityEducation@intel.com**.

Intel and the Intel and McAfee logos are trademarks of Intel Corporation or McAfee, Inc. in the US and/or other countries. Other marks and brands may be claimed as the property of others. Copyright © 2016 Intel Corporation. 1839_1016
OCTOBER 2016

McAfee. Part of Intel Security.
2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com